



*One League, One Focus - Your Success!*

## **Memorandum**

**TO: Members of Wisconsin Legislature**

**FROM: The Wisconsin Credit Union League**

**DATE: February 19, 2008**

**RE: Support Senate Bill 439 and Assembly Bill 745 – Plastic Card Data Security Legislation**

On behalf of our 260 member credit unions and their 2.1 million member-owners, The Wisconsin Credit Union League respectfully requests your support for SB 439 and AB 745 and encourages adoption of the legislation this session.

In many recent well-publicized instances, companies have taken sensitive data from consumers' credit and debit cards and then have lost or misused it after completing transactions.. This collection, mishandling, and subsequent misuse of the data costs consumers and their financial institutions hundreds of millions of dollars each year.

SB 439 and AB 745 directly address this significant problem. The proposals will protect consumers and their financial institutions by limiting careless business' ability to collect and keep sensitive data held on credit and debit cards after transactions have been completed.

The proposals are totally consistent with payment card industry data security standards for the handling of sensitive data. It does not, nor is it intended to, interfere with transactions in way. It only limits the collection of data not needed after a transaction is complete.

Thank you for supporting this timely and greatly needed consumer legislation. If you haven any questions, please do not hesitate to contact us.

N25 W23131 Paul Road Pewaukee, Wisconsin 53072-5779

Phone: (262) 549-0200 or (800) 242-0833 Fax: (262) 549-7722 Web: [www.theleague.coop](http://www.theleague.coop)

Member Credit Union National Association

For Immediate Release  
Jan. 25, 2008

Contact: Chris Olson  
(800) 242-0833, Ext. 3167  
[colson@theleague.coop](mailto:colson@theleague.coop)  
[www.theleague.coop](http://www.theleague.coop)

## **Credit unions support legislative proposal on personal data security**

**Pewaukee, Wis.** - Wisconsin credit unions support draft legislation introduced by State Rep. Brett Davis (R-Oregon) and State Sen. Bob Wirth (D-Pleasant Prairie) that would keep safer personal information stored on credit and debit cards.

"Due to recent breaches of consumers' personal information involving payment cards, legislators and consumers have a heightened awareness of the extremely important matter of data security. We hope this common sense proposal will win broad bi-partisan support and be signed into law this session," says Brett Thompson, President & CEO of The Wisconsin Credit Union League, the trade association representing 260 not-for-profit, member-owned financial institutions. "Sen. Wirth and Rep. Davis deserve much credit for their leadership in addressing this issue which, if not addressed immediately, could sharply erode consumer confidence in plastic payment cards."

LRB 2983 is the bill draft that would prohibit merchants from retaining PINs or security codes after processing a credit or debit card transaction. If a merchant were to ignore the law and collect and keep that information and if the information were lost, the party responsible for losing the information would be required to pay for the costs to close consumers' accounts and re-issue cards. The party responsible for the loss would also be required to pay for steps that intend to prevent any ensuing fraudulent use of a consumer's personal information and cover certain costs enabling continued financial services to the card holder, such as notifying affected customers or crediting accounts for fraudulent transactions.

Thompson says an overwhelming majority – around 75% – of Wisconsin consumers responding to a January telephone poll conducted on behalf of The League support measures that require the party responsible for a data breach to bear such restorative costs. He says consumers may spend up to 60 hours to fix damage caused by a breach and attempts at fraud.

"To allow consumer data to live in vulnerable environments where the information might be used beyond its intended purpose is nothing short of an invitation for fraud," Thompson says.

"This bill follows some of the payment card industry's existing, basic rules that merchants sometimes ignore since they don't carry the force of law or have any real consequence for those who ignore the rules," Thompson adds. "The payment card system itself acknowledges the imprudence of storing sensitive personal information when it's unnecessary to do so."

He also suggests that improved data security would improve consumer confidence in spending, stimulating the economy.

Credit unions, which are member-owned cooperatives, have a more difficult time offering attractive rates on savings and loans to members when they must bear the costs related to breaches of personal information.

– END –

N25 W23131 Paul Road, Pewaukee, WI 53072-5779

Credit unions are cooperative financial institutions that are owned by their members and do not have stockholders. Because they are not-for-profit, they return earnings to members in the form of more competitive rates of return on accounts, lower interest on loans, lower fees and improved services. Around 2.1 million Wisconsin residents belong to credit unions, of which nearly half are open to the local community. People can find a credit union to join by looking in the phone book or by visiting [www.creditunion.coop](http://www.creditunion.coop).

Please Support:  
The Plastic Card Data Security Bills –  
Assembly Bill 745 (Rep. Davis) and Senate Bill 439 (Sen. Wirsch)

**What do the bills do?**

Prohibits a company from retaining sensitive information when a customer uses a credit or debit card. The information includes security codes and personal identification numbers. An individual in violation must reimburse the consumer and financial institution that issued the card for the cost of reasonable actions taken to protect personal information such as canceling and reissuing cards.

**Why is legislation necessary?**

- **Data breaches have increased.** This legislation protects consumers from credit and debit card fraud and the high costs associated with a data breach.
- **Costs to business are high.** According to CUNA Mutual Group, losses to American credit unions and their members due to credit and debit card fraud was nearly \$100 million in 2006.
- **Financial and credit information is sensitive.** A consumer spends 15 to 60 hours to fix the damage caused by a breach of his or her financial information and the subsequent attempts at fraud.
- **Fraud adds to the cost of lending.** The cost of canceling and re-issuing cards due to data breaches increase costs and makes it more difficult to offer attractive rates on day-to-day services, like saving accounts and loans.
- **Some retailers retain financial information.** Under the legislation, companies may not keep pins or security codes held on magnetic strips of cards after a transaction is complete. 75% of Wisconsin consumers responding to a January telephone poll support this measure.
- **Secure retailers are exempt.** A business is exempt from the prohibitions of this legislation if it complies with certain federal privacy and security standards or with certain industry standards for data encryption and security.

January 23, 2008

To: All Legislative Offices  
From: Senator Bob Wirch and Representative Brett Davis  
Re: LRB 2983 – Payment Card Users Protection Bill

Dear Colleagues,

Yesterday, constituents may have asked you to co-sponsor important consumer protection legislation that would be shortly forthcoming. Below is the co-sponsorship memo for the legislation they were referencing.

In the U.S. in 2006, \$56.6 billion were stolen through identity theft, with an average fraud per victim of \$6,278. Much of these losses are covered by businesses. In 2004, businesses reported average monetary losses of \$49,254.

It's estimated that consumers who are victims of credit card fraud/I.D. theft spend an average of 15 – 60 hours attempting to repair damage to their name from the fraud. The last few years alone, the estimated total number of records containing sensitive personal information involved in security breaches in the U.S. is a staggering 217,393,476.

While there are many facets to the challenges we face in limiting identification theft and fraud it's clear that keeping sensitive or personal information from being lost in a data breach of some kind will help protect consumers.

Well publicized data breaches such as the one TJX Companies Inc. (TJMaxx and Marshalls) experienced, should not be allowed to happen again. In that instance, data was legally taken and kept from consumer's credit and debit cards, but was stolen.

We propose to strengthen consumer protection by limiting the amount of time a business can retain certain information in a transaction where a consumer uses their credit or debit card. Carelessness on the part of individuals who accept credit and debit cards will continue to place significant burdens on consumers and costs financial institutions unless the attached legislation is adopted.

Please call either Rep. Davis at 6-1192 or Sen. Wirch at 7-8979 office to co-sponsor this important legislation – LRB 2983/1 - by January 30<sup>th</sup>.

Note: This bill does not apply to rewards, awards or points type programs that businesses engage in and issue plastic cards for.

Statement of Joe Dillon  
CUNA Mutual Group  
S.B. 439, Data Security  
Wisconsin Senate Committee on Veterans and Military Affairs,  
Biotechnology and Financial Institutions  
February 20, 2008

Chairman and Members of the Committee,

Thank you for the opportunity to appear before you today in support of S.B. 439 and to present our experience with losses due to theft from data security fraud.

I am Joe Dillon, a vice president with CUNA Mutual Group, one of the few companies to provide commercial insurance for theft from data security losses, most commonly referred to as plastic card losses. CUNA Mutual is headquartered in Madison, Wisconsin, with more than 2000 employees in the state and is the premier insurer of credit unions.

Credit unions, which represent about 6% of the financial services market consisting of banks, thrifts and credit unions, have experienced a dramatic growth in theft from plastic card losses over the last few years. Other financial institutions have experienced similar growth patterns in theft from plastic card fraud.

What I will relate is the trend we have seen over the last six years for reported plastic card losses. It does not include losses that went unreported because they were less than the institution's deductible:

- In 2002, credit unions filed claims for \$39 million in plastic card losses.

- In 2003 that amount grew to \$40 million. And then we began to see a sharp increase in reported plastic card losses:
- \$57 million in 2004 to
- \$89 million in 2005 (a 56% increase), and
- \$98.7 million in 2006 (an 11% increase).

In 2007, actual credit union submitted losses reported to CUNA Mutual totaled \$72.6 million – down from the record losses of \$98.7 million in 2006. Despite this improvement, it is still the third worst year of submitted losses.

We believe that some of this decrease is attributed to changes in our insurance coverage. Because we have raised aggregate and per-card deductibles in 2007, comparison between 2006 and 2007 becomes more problematic. Consequently, we are now comparing apples to oranges when we look at raw submitted loss data.

These losses are from actual theft by fraudulent activities. They do not include the cost of notifying consumers that their card has been compromised, nor do they include the cost of issuing replacement cards when necessary.

We estimate that eighty-one (81) percent of the reported plastic card losses are attributed to theft of credit and debit card data that was retained in an unsafe format by merchants and subsequently breached.

While the fraud losses sustained by credit unions continues to remain high, plastic card data breaches reached an all-time record high in 2007. In 2007, more than 103 million credit and debit cards were breached including the 94 million cards

compromised in the massive TJX data breach. As a result, the plastic card environment remains extremely volatile.

To recover some of these losses, we filed suit in 2005 in the BJ Wholesalers case to recover up to \$8 million in direct fraud losses for ourselves and credit unions.

To date, the only decisions reached by the court in the BJ's matter are to dismiss the claims that have been filed, and those claims were filed largely by banks. First, our negligence claims were dismissed based upon the economic loss doctrine. Second, our breach of contract claims were dismissed because of the way in which the contracts are set up by VISA and MasterCard. Unfortunately, the court rejected the card issuing banks' and credit unions' allegations that they are third party beneficiaries of the contracts between the merchants and the acquiring financial institutions, and between the acquiring financial institutions and VISA. In other words, there is no contract between the credit union and the merchant to enforce.

Our only remaining claims in the BJ Wholesalers case are claims of misrepresentation under common law and the Massachusetts Unfair Trade Practices statute. Those claims have survived, but have not been decided.

At the end of 2007, many financial institutions entered into a \$40.9 million settlement with TJX/VISA for their losses. The payouts in these individual cases represented a small percentage of the actual losses. As a result, a number of financial institutions, including credit unions, rejected the settlement even though a U.S. District Court denied a request for class action certification. Presently the case resides in Massachusetts State Court.

When examining the financial chain for a data breach, it is easy to see why certain entities have been slow in following best practices and card association rules – the legal and financial consequences are limited. They are not the party that sends out the breach notice for their mistake (the issuer of the credit card is responsible) and their legal exposure is very low. To date, no court has ruled that a card issuing credit union or bank may recover its losses.

As a result, S.B. 439 addresses the growing problem of data security fraud by simply stipulating that:

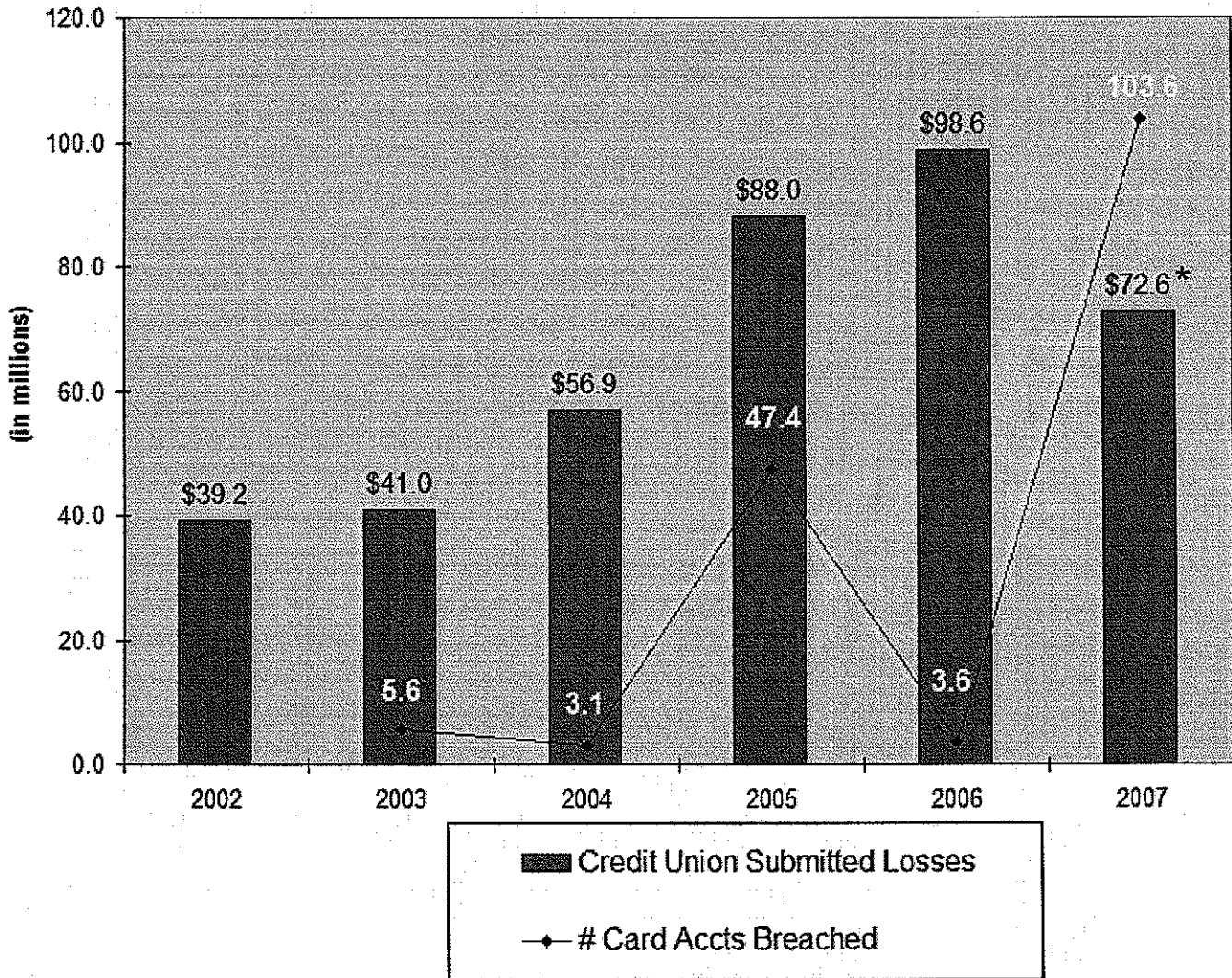
- 1) Entities may not retain sensitive credit information, and
- 2) The entity that fails to protect such information accepts responsibility for the expense of notifying consumers when their credit and debit card information has been breached, for replacing the cards when necessary, and the resulting fraud.

We believe these fair and reasonable steps will significantly improve the safety of Wisconsin consumers' sensitive credit and debit card information.

Thank you. I will be pleased to answer your questions.



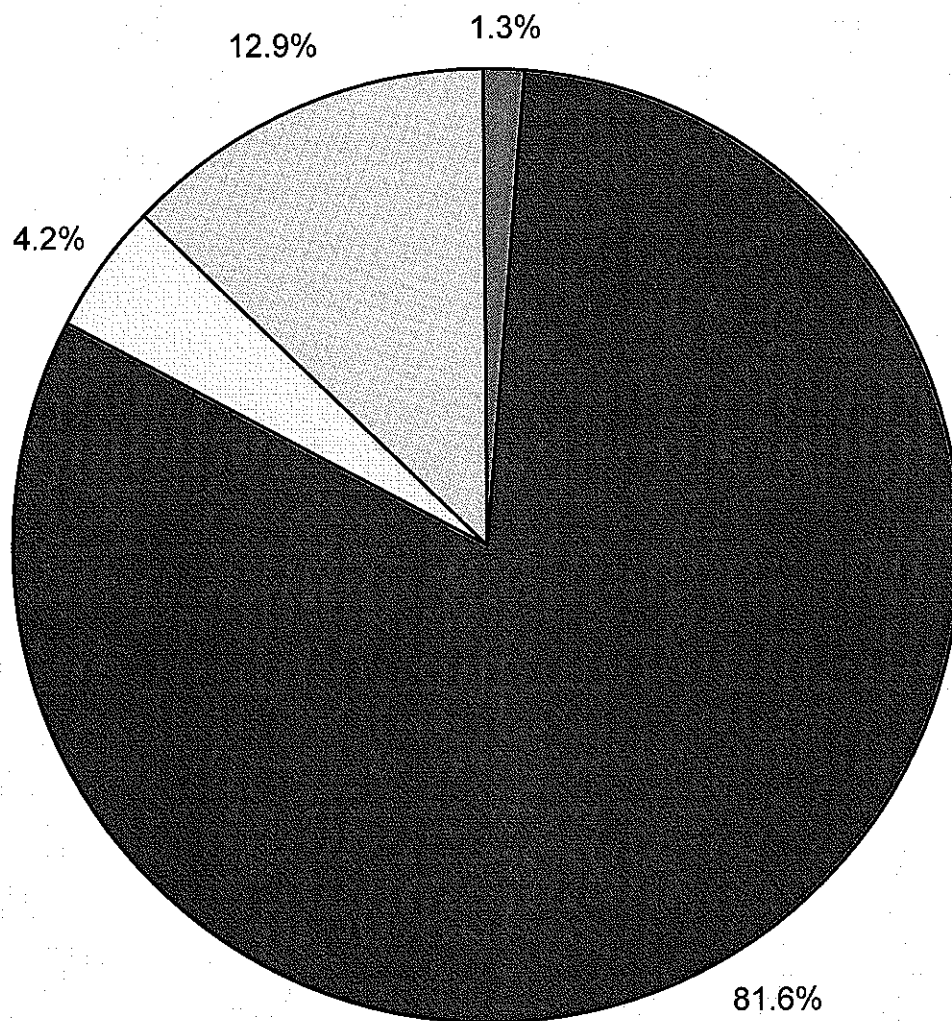
**Submitted Dollars of Plastic Card Losses to CUNA Mutual  
&  
Card Accounts Breached Industry Wide**



\*CUNA Mutual increased policyholder deductibles resulting in a change in the reporting of credit unions submitted losses. We believe actual losses are greater in 2007.

## 2007 Submitted Credit Union Losses by Fraud Type

Other Counterfeit Lost Stolen Card



## Data Breach Impact Chain

Entity Affected By A Data Breach	Impacts
Cardholder/Credit union Member	Legally responsible for \$50 on credit cards but this is mostly waived Identity theft risk Inconvenience/Embarrassment Stops using the card
Financial Institution Issuer/ Credit Union	Retain losses caused by fraudulent transactions Reissue card expenses Overhead expenses (projected at \$130 - \$185 per account) Cardholder stops using the card resulting in lose of revenue Cardholder account closures Increase insurance costs and deductibles
Insurer/CUNA Mutual	Pay Financial institution for qualified losses Increase rates attributed to data breaches
Processor for the Financial Institution Issuer	None: Expenses passed to the Financial Institution Issuer/Credit Union
Associations: Visa, MasterCard, American Express, Discover	None: Expense passed to Financial Institution Issuer/Credit Union Rule enforcement governing the payment system Authority to levy fines on Merchant Processors in violation of regulations
Merchant Processor	Possible fines levied by Associations on Merchant Processor for not following regulations.
Merchant	Litigation expenses Association fines